

**ELECTRONIC WATERMARK COMPOSITING DEVICE AND IMAGE ALTERATION DECIDING DEVICE**

Patent Number: JP2001078013  
Publication date: 2001-03-23  
Inventor(s): ARAGAI YASUHIRO; TAKENAKA YUJI  
Applicant(s): FUJI PHOTO FILM CO LTD  
Requested Patent: ☐ JP2001078013  
Application Number: JP19990250297 19990903  
Priority Number(s):  
IPC Classification: H04N1/387; G06T1/00; G09C1/00; G09C5/00; H04L9/32  
EC Classification:  
Equivalents:

---

**Abstract**

---

**PROBLEM TO BE SOLVED:** To composite an electronic watermark with an image photographed by an order receiver based on the request of an orderer by compositing cipher information which is prepared by enciphering image identification information for identifying an input image with the image as an electronic watermark, recording it and reporting a method thereof and the image identification information.

**SOLUTION:** A method for extracting the electronic watermark composited with an image 10, a method for deciphering the cipher information to be used as electronic watermark and the image identification information of the image 10 to be used for preparing the cipher information are reported by the manager of a laboratory system to the user of an image alteration discriminating device 90, namely, to the orderer. The order receiver receives a recording medium such as CD-ROM storing a composited image 11 from a laboratory system, selects a required image out of recorded images and presents it to the orderer as photograph data for proving progress. In order to discriminate whether an image 12 presented by the order receiver is altered, the orderer uses the image alteration discriminating device 90.

---

Data supplied from the esp@cenet database - I2

(19)日本国特許庁(JP)

## (12)公開特許公報 (A)

(11)特許出願公開番号

特開2001-78013

(P2001-78013A)

(43)公開日 平成13年3月23日(2001.3.23)

(51)Int. Cl. <sup>7</sup>		識別記号		F I		テ-マ-ト*(参考)	
H 0 4 N	1/387			H 0 4 N	1/387		5B057
G 0 6 T	1/00			G 0 9 C	1/00	6 4 0 B	5C076
G 0 9 C	1/00	6 4 0				6 4 0 D	5J104
					5/00		
	5/00			G 0 6 F	15/66	B	
審査請求	未請求	請求項の数	1 1	O L		(全 1 0 頁)	最終頁に続く

(21)出願番号 特願平11-250297

(22)出願日 平成11年9月3日(1999.9.3)

(71)出願人 000005201

富士写真フィルム株式会社

神奈川県南足柄市中沼210番地

(72)発明者 新貝 安浩

東京都港区西麻布2丁目26番30号 富士写真フィルム株式会社内

(72)発明者 竹中 裕二

東京都港区西麻布2丁目26番30号 富士写真フィルム株式会社内

(74)代理人 100104156

弁理士 龍華 明裕

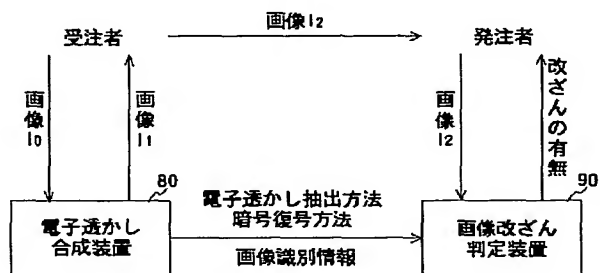
最終頁に続く

(54)【発明の名称】電子透かし合成装置及び画像改ざん判定装置

## (57)【要約】

【課題】 画像に電子透かしを合成する画像合成装置、及び画像の改ざんの有無を判定する画像改ざん判定装置を提供する。

【解決手段】 画像を入力する画像入力部と、画像を識別する画像識別情報を暗号化した暗号情報を作成する暗号作成部と、暗号情報を電子透かしとして画像に合成する電子透かし合成部と、電子透かし合成部によって合成された画像を記録する画像記録部と、電子透かしの抽出方法、暗号情報の復号方法、及び画像識別情報を通知する画像情報通知部とを備えた。



## 【特許請求の範囲】

【請求項1】 画像に電子透かしを合成する電子透かし合成装置であって、  
前記画像を入力する画像入力部と、  
前記画像を識別する画像識別情報を暗号化した暗号情報を作成する暗号作成部と、  
前記暗号情報を電子透かしとして前記画像に合成する電子透かし合成部と、  
前記電子透かし合成部によって合成された画像を記録する画像記録部と、  
前記電子透かしの抽出方法、前記暗号情報の復号方法、及び前記画像識別情報を通知する画像情報通知部とを備えたことを特徴とする電子透かし合成装置。

【請求項2】 前記暗号作成部は、公開鍵暗号系における秘密鍵に基づいて、前記画像識別情報のデジタル署名を作成することによって、前記暗号情報を作成することを特徴とする請求項1に記載の電子透かし合成装置。

【請求項3】 前記画像識別情報は、前記画像の記録の依頼者毎に異なる識別情報であることを特徴とする請求項2に記載の電子透かし合成装置。

【請求項4】 前記画像識別情報は、前記画像の記録の注文毎に異なる識別情報であることを特徴とする請求項2に記載の電子透かし合成装置。

【請求項5】 前記画像識別情報は、前記画像毎に異なる識別情報であることを特徴とする請求項2に記載の電子透かし合成装置。

【請求項6】 画像の改ざんの有無を判定する画像改ざん判定装置であって、  
前記画像を入力する画像入力部と、  
前記画像の電子透かし抽出方法、前記電子透かしの暗号を復号する暗号復号方法、及び前記画像を識別する画像識別情報を入力する画像情報入力部と、  
前記電子透かし抽出方法に基づいて、前記画像の電子透かしを抽出する電子透かし抽出部と、  
前記暗号復号方法に基づいて、前記電子透かしの復号する暗号復号部と、  
前記暗号復号部が復号した復号データと、前記画像識別情報とを比較することにより、前記画像の改ざんの有無を判定する改ざん判定部とを備えたことを特徴とする画像改ざん判定装置。

【請求項7】 前記暗号復号部は、前記電子透かしをデジタル署名とみなし、公開鍵暗号系における公開鍵に基づいて前記デジタル署名を復号化することによって、前記復号データを得ることを特徴とする請求項6に記載の画像改ざん判定装置。

【請求項8】 前記画像識別情報は、前記画像の撮影者毎に異なる識別情報又は前記画像毎に異なる識別情報であることを特徴とする請求項7に記載の画像改ざん判定装置。

【請求項9】 画像の改ざんの有無を判定する画像改ざ

ん判定方法であって、

前記画像を入力し、

前記画像の電子透かし抽出方法、前記電子透かしの暗号を復号する復号方法、前記画像を識別する識別情報を入力し、

前記電子透かし抽出方法に基づいて、前記画像の電子透かしを抽出し、

前記復号方法に基づいて、前記電子透かしの復号して復号データを抽出し、

10 前記復号データと、前記画像識別情報とを比較することにより、前記画像の改ざんの有無を判定することを特徴とする画像改ざん判定方法。

【請求項10】 前記画像の前記識別情報は、前記画像の撮影者毎に異なる識別情報又は前記画像毎に異なる識別情報であることを特徴とする請求項9に記載の画像改ざん判定方法。

【請求項11】 画像の改ざんの有無を判定するコンピュータ用のプログラムを格納した記録媒体であって、前記プログラムが、

20 前記コンピュータに前記画像を入力させる画像入力モジュールと、

前記コンピュータに、前記画像の電子透かし抽出方法、前記電子透かしの暗号を復号する復号方法、前記画像を識別する画像識別情報を入力させる画像情報入力モジュールと、

前記電子透かし抽出方法に基づいて、前記画像の電子透かしを抽出させる電子透かし抽出モジュールと、  
前記復号方法に基づいて、前記電子透かしの復号化させる暗号復号モジュールと、

30 前記暗号復号モジュールが復号した復号データと、前記画像識別情報とを比較することにより、前記画像の改ざんの有無を判定させる改ざん判定モジュールとを備えたことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、画像に電子透かしを合成する画像合成装置及び画像の改ざんの有無を判定する画像改ざん判定装置に関する。

【0002】

40 【従来の技術】工事現場において、工事の受注者は、工事の出来高を説明するために、工事の段階ごとに工事現場の写真を撮影し、工事の発注者に提出し、工事が正しく実施されたことを報告する。

【0003】工事写真をAPSカメラまたはデジタルカメラで撮影した場合、デジタル画像データをCD-ROM等の電子媒体で提出することが行われる。しかしデジタル画像データは、コンピュータ等のソフトウェアによって容易にデータを変更することができるため、工事の受注者がデータを改ざんする可能性がある。そのため、工事の発注者が、工事の受注者が提出した画像データに

改ざんがないことを判定する方法が必要である。

【0004】画像データの改ざんの有無を判定する発明として、特開平11-98344号公報（公開日1999年4月9日）には、予め原画像及びその原画像に埋め込んだ透かし画像を記憶し、改ざんされた可能性のある合成画像を入力した際、合成画像と原画像の差分を検出することにより、合成画像に埋め込まれた透かし画像を抽出し、予め登録された透かし画像と比較して、改ざんの有無を判定する改ざん判定方法及び装置が開示されている。

【0005】

【発明が解決しようとする課題】しかしながら、上記の発明においては、改ざん判定装置が、予め原画像を記憶する必要があるため、工事写真のように数多くの画像の改ざんの判定を行わなければならない場合、原画像を記憶するための記憶容量が大きくなるという問題を生じる。

【0006】そこで本発明は、上記の課題を解決するために、発注者の依頼に基づいて受注者が撮影した画像に電子透かしを合成する画像合成装置、及び受注者が発注者に提出する画像の改ざんの有無を判定する画像改ざん判定装置を提供することを目的とする。この目的は特許請求の範囲における独立項に記載の特徴の組み合わせにより達成される。また従属項は本発明の更なる有利な具体例を規定する。

【0007】

【課題を解決するための手段】上記課題を解決するために、本発明の第1の形態においては、画像に電子透かしを合成する電子透かし合成装置であって、画像を入力する画像入力部と、画像を識別する画像識別情報を暗号化した暗号情報を作成する暗号作成部と、暗号情報を電子透かしとして画像に合成する電子透かし合成部と、電子透かし合成部によって合成された画像を記録する画像記録部と、電子透かしの抽出方法、暗号情報の復号方法、及び画像識別情報を通知する画像情報通知部とを備えたことを特徴とする。

【0008】暗号作成部は、公開鍵暗号系における秘密鍵に基づいて、画像識別情報のデジタル署名を作成することによって、暗号情報を作成してもよい。

【0009】画像識別情報は、画像の記録の依頼者毎に異なる識別情報であってもよい。画像識別情報は、画像の記録の注文毎に異なる識別情報であってもよい。画像識別情報は、画像毎に異なる識別情報であってもよい。

【0010】本発明の第2の形態においては、画像の改ざんの有無を判定する画像改ざん判定装置であって、画像を入力する画像入力部と、画像の電子透かし抽出方法、電子透かしの暗号を復号する暗号復号方法、及び画像を識別する画像識別情報を入力する画像情報入力部と、電子透かし抽出方法に基づいて、画像の電子透かしを抽出する電子透かし抽出部と、暗号復号方法に基づい

て、電子透かしを復号する暗号復号部と、暗号復号部が復号した復号データと、画像識別情報とを比較することにより、画像の改ざんの有無を判定する改ざん判定部とを備えたことを特徴とする。

【0011】暗号復号部は、電子透かしをデジタル署名とみなし、公開鍵暗号系における公開鍵に基づいてデジタル署名を復号化することによって、復号データを得てもよい。

【0012】画像識別情報は、画像の撮影者毎に異なる識別情報又は画像毎に異なる識別情報であってもよい。

【0013】本発明の第3の形態においては、画像の改ざんの有無を判定する画像改ざん判定方法であって、画像を入力し、画像の電子透かし抽出方法、電子透かしの暗号を復号する復号方法、画像を識別する識別情報を入力し、電子透かし抽出方法に基づいて、画像の電子透かしを抽出し、復号方法に基づいて、電子透かしを復号して復号データを抽出し、復号データと、画像識別情報とを比較することにより、画像の改ざんの有無を判定することを特徴とする。

【0014】画像の識別情報は、画像の撮影者毎に異なる識別情報又は画像毎に異なる識別情報であってもよい。

【0015】画像の改ざんの有無を判定するコンピュータ用のプログラムを格納した記録媒体であって、プログラムが、コンピュータに画像を入力させる画像入力モジュールと、コンピュータに、画像の電子透かし抽出方法、電子透かしの暗号を復号する復号方法、画像を識別する画像識別情報を入力させる画像情報入力モジュールと、電子透かし抽出方法に基づいて、画像の電子透かしを抽出させる電子透かし抽出モジュールと、復号方法に基づいて、電子透かしを復号化させる暗号復号モジュールと、暗号復号モジュールが復号した復号データと、画像識別情報とを比較することにより、画像の改ざんの有無を判定させる改ざん判定モジュールとを備えたことを特徴とする。

【0016】なお上記の発明の概要は、本発明の必要な特徴の全てを列挙したものではなく、これらの特徴群のサブコンビネーションも又発明となりうる。

【0017】

【発明の実施の形態】以下、発明の実施の形態を通じて本発明を説明するが、以下の実施形態は特許請求の範囲にかかる発明を限定するものではなく、また、実施形態の中で説明されている特徴の組み合わせの全てが発明の解決手段に必須であるとは限らない。

【0018】以下、本発明を工事写真の例を用いて説明するが、本発明は工事写真に限らず、一般にデジタル画像データに電子透かしを合成し、改ざんの有無を判定することを目的として利用することができる。

【0019】図1は、本発明の電子透かし合成装置80と画像改ざん判定装置90を用いて、工事の受注者が納

品した工事写真のデジタル画像が改ざんされているかどうかを、工事の発注者が判定することのできるシステムの構成図である。

【0020】電子透かし合成装置80は、銀塩フィルム、APS (Advanced Photo System) フィルム、デジタルカメラの画像を記録した半導体メモリ等から画像データを読み取り、CD-ROMなどの媒体にデジタル化した画像を記録する。通常、電子透かし合成装置80は、写真の現像サービスを提供するラボシステムにおいて、ラボシステムの従業員が使用する。

【0021】工事の受注者は、銀塩フィルム、APS (Advanced Photo System) フィルム、半導体メモリ等に記録された、写真の原画像I0をラボシステムに提供する。ラボシステムの従業員は原画像I0を電子透かし合成装置80に入力する。

【0022】電子透かし合成装置80は、写真I0をデジタル化し、写真I0を識別する画像識別情報に基づいて、暗号情報を作成し、作成された暗号情報を電子透かしとして画像I0に合成する。電子透かし合成装置80は合成された画像I1をCD-ROM等に記録して、受注者に提供する。

【0023】合成画像I1は、肉眼では原画像I0と区別がつかないため、受注者が合成画像I1から電子透かしを検出することは困難である。

【0024】電子透かし合成装置80において、画像I0に合成された電子透かしの抽出方法、電子透かしとして使用された暗号情報の復号方法、及び暗号情報の作成に用いた画像I0の画像識別情報は、ラボシステムの管理者によって、画像改ざん判定装置90の使用者、すなわち工事の発注者に通知される。通知手段は、郵便や電子メールなどを用いることができる。

【0025】受注者は、ラボシステムから合成画像I1が格納されたCD-ROM等の記録媒体を受け取り、CD-ROM等に記録された画像の中から必要な画像を選んで工事の進捗を証明する写真データとして発注者に提出する。発注者に提出された画像は、合成画像I1に対応する画像I2であるとし、受注者は画像I1を改ざんして画像I2を作成した可能性があるとする。

【0026】発注者は、受注者が提出した画像I2に改ざんがあるかどうかを判定するため、画像改ざん判定装置90を用いる。画像改ざん判定装置90には予め画像I1の電子透かし抽出方法と、暗号復号方法と、画像識別情報が入力されている。画像改ざん判定装置90は画像I2を入力し、画像I1の電子透かし抽出方法により、画像I2の電子透かしの抽出する。抽出した電子透かしの暗号情報とみなし、画像I1の暗号復号方法により、復号する。さらに、復号されたデータと画像I1の画像識別情報を比較し、一致するなら画像I2は画像I1から改ざんされていないと判定し、一致しないなら画像I2は画像I1から改ざんされたと判定する。

【0027】図2は、本発明の第1の実施形態に係る電子透かし合成装置80の構成図である。電子透かし合成装置80は、画像入力部10と、処理部20と、記録部40と、出力部50とを有する。

【0028】画像入力部10は、画像を入力する。銀塩カメラで撮影された画像を画像処理装置に入力する場合、画像入力部10には、ネガフィルムやポジフィルム等の写真フィルム上の画像を光学的に走査して電気信号に変換するフィルムスキャナが用いられる。デジタルカメラで撮影されたデジタル画像を画像処理装置に入力する場合、画像入力部10には、入力するデジタル画像を格納した記録媒体に応じた各種読取装置が用いられる。例えば、画像入力部10には、不揮発性の半導体メモリカード等の着脱自在な記録媒体から画像データを読み取るための読取装置等が用いられる。また、フロッピーディスク、MO、CD-ROM等から画像データを読み取る場合は、画像入力部10としてそれぞれフロッピードライブ、MOドライブ、CDドライブ等が用いられる。

【0029】処理部20は、暗号情報を作成し、画像入力部10が入力した画像に暗号情報を電子透かしとして合成する。処理部20の詳細な構成及び動作は後述する。

【0030】記録部40は、処理部20から受け取った画像を着脱自在な記録媒体に記録する。記録媒体としては、書き込み可能なCD、DVD等の光記録媒体や、MO等の光磁気記録媒体、フロッピー（登録商標）ディスク等の磁気記録媒体等が考えられる。記録部40としては、CD-Rドライブ、DVDドライブ、MOドライブ、フロッピードライブ等が用いられる。なお、記録部40は、半導体メモリ等の記憶装置に画像を記録してもよい。

【0031】出力部50は、処理部20から受け取った画像を出力する。例えば画像を画面表示する場合、出力部50には画像を表示するモニタが用いられる。

【0032】次に、処理部20が作成する暗号情報について説明する。暗号情報の作成には、たとえば公開鍵暗号方式を用いたデジタル署名を用いることができる。

【0033】公開鍵暗号方式は、暗号鍵と復号鍵が異なり、暗号鍵を公開し、復号鍵を秘密にする。公開された暗号鍵を公開鍵と呼び、秘密にされた復号鍵を秘密鍵と呼ぶ。一方、デジタル署名とは、通信文が改ざんされていないこと及びその通信文の送信者が偽者ではないことを認証する機能である。以下、公開鍵暗号方式を用いたデジタル署名の実現方法を説明する。

【0034】通信文Mに対して、公開鍵pkを用いて暗号化関数Eによって暗号化したデータをE(M, pk)とする。また通信文Mに対して、秘密鍵skを用いて復号化関数Dによって復号化したデータをD(M, sk)とする。

【0035】公開鍵暗号方式において、公開鍵pk、暗

10

20

30

40

50

号化関数Eが与えられたとき、暗号化データE (M, p k) を求めることは容易である。また秘密鍵s k、復号化関数Dが与えられたとき、復号化データD (M, s k) を求めることは容易である。

【0036】公開鍵p k、暗号化関数Eは誰もが知っているため、全ての通信文Mに対して、暗号化データE (M, p k) を容易に計算できるが、秘密鍵s kを知らなければ、暗号化データE (M, p k) から通信文Mを復元することはできない。すなわち、暗号化関数Eの逆関数である復号化関数Dを求めることは計算量の点で困難である。

【0037】秘密鍵s kと復号化関数Dを知っているなら、暗号化データE (M, p k) に対して、秘密鍵s kを用いて復元関数Dによって、D (E (M, p k), s k) の値を求めることにより、容易に通信文Mを復元することができる。すなわち、式

$$M = D(E(M, pk), sk)$$

が成立する。

【0038】公開鍵暗号方式を用いてデジタル署名を実現するには、公開鍵暗号方式の暗号化、復号化の操作を逆に用いる。公開鍵暗号方式においては、暗号化と復号化を逆に用いて、復号化関数によって通信文を暗号化し、暗号化関数によって暗号化された通信文を復号化することができる。

【0039】通信文Mの送信者は、秘密鍵s kと復号化関数Dを知っているとする。送信者通は、通信文Mを秘密鍵s kと復号化関数Dによって暗号化する。暗号化された通信文はD (M, s k) である。これを通信文Mのデジタル署名と言う。通信文Mの送信者は、通信文Mとともに、通信文Mのデジタル署名D (M, s k) を通信の受信者に送信する。

【0040】受信者は、公開鍵p kを用いて暗号化関数Eによって暗号化データD (M, s k) を復号化する。復号化されたデータはE (D (M, s k), p k) である。通信の途中で通信文Mやデジタル署名D (M, s k) が改ざんされていない限り、復号化されたデータE (D (M, s k), p k) の値はMに一致する。すなわち式

$$M = E(D(M, sk), pk)$$

が成立する。

【0041】仮に、通信文MがM\*に改ざんされたとすれば、デジタル署名を復号化したデータE (D (M, s k), p k) はMになるが、受信した通信文はM\*である。すなわち、式

$$M^* \neq M = E(D(M, sk), pk)$$

が成立する。したがって、デジタル署名の復号結果と受信した通信文が異なることから、通信文が改ざんされたことを知ることができる。

【0042】ここで、D (M, s k) の計算ができるのは、秘密鍵s kを知っているのは通信文の送信者本人だ

けである。したがって、第3者が通信文MをM\*に改ざんした後に、通信文M\*に対するデジタル署名D (M\*, s k) を作成することは不可能である。すなわち、通信文Mを改ざんするとともに、それに合わせてデジタル署名を改ざんして、改ざんを隠蔽することはできない。

【0043】また、通信の受信者と同じ公開鍵暗号系で通信を行う他人が、通信文Mの送信者になりすまして、デジタル署名を作成することはできない。なぜなら、秘密鍵s kは通信部Mの送信者しか知らないため、他人が通信文Mのデジタル署名D (M, s k) を作成することはできないからである。仮に、他人が異なる秘密鍵s k\*と復号化関数Dを用いて求めた、通信文Mのデジタル署名D (M, s k\*)を通信文Mとともに通信の相手に送ると、通信の受信者は、デジタル署名D (M, s k\*)を試みる。復元された通信文はE (D (M, s k\*), p k) であるが、これは通信文Mには一致しない。すなわち、式

$$M \neq E(D(M, sk^*), pk)$$

が成立する。したがって、他人が通信文Mの送信者になりすまして、通信文Mを送信したことを検出することができる。

【0044】以上述べたように、公開鍵暗号方式を用いることにより、デジタル署名を実現できる。すなわち通信文の改ざんがなされていないこと、他人が通信文の真の送信者になりすまして通信文を送信していないことを認証することができる。尚、公開鍵暗号、デジタル署名については、「暗号理論入門」(岡本栄司著、共立出版)に詳しい。

【0045】本実施形態の電子透かし合成装置80では、上述の通信文Mとして、画像識別情報IDを用い、画像識別情報IDのデジタル署名を作成し、電子透かしとして画像に合成する。

【0046】画像識別情報IDは、たとえば受注者を識別する受注者識別情報、受注者がラボシステムに画像のデジタル化を依頼したときの注文を識別する注文識別情報、画像入力部10が入力した画像を識別する画像毎の識別情報のいずれであってもよい。

【0047】図3は、本実施形態の電子透かし合成装置80の処理部20の機能ブロック図である。処理部20は、暗号作成部22と、電子透かし合成部24と、画像情報通知部26とを有する。

【0048】暗号作成部22は、公開鍵暗号系の秘密鍵及び画像識別情報IDを用いて、暗号情報の一例としてデジタル署名を作成する。当該電子透かし合成装置80を使用するラボシステムの管理者と工事の発注者の間では公開鍵暗号が用いられ、秘密鍵は、ラボシステムの管理者が秘匿し、公開鍵は発注者に知らされる。

【0049】電子透かし合成部24は、暗号作成部22が作成したデジタル署名を電子透かしとして画像入力部

10が入力した画像に合成する。

【0050】画像識別情報IDが、受注者識別情報である場合、同一の受注者であれば、画像入力部10が入力した画像のすべてに同一のデジタル署名が作成され、電子透かしとして埋め込まれる。

【0051】画像識別情報IDが、注文識別情報である場合、同一の受注者であっても、注文単位毎に異なるデジタル署名が作成され、電子透かしとして埋め込まれる。

【0052】画像識別情報IDが、画像毎に異なる識別情報である場合、画像入力部10が入力した画像毎に異なるデジタル署名が作成され、電子透かしとして埋め込まれる。

【0053】画像毎に異なる画像識別情報IDの例としては、たとえば、ランダムに生成した画像のファイル名であってもよい。また、画像データの一部分を取り出して、画像識別情報IDとしてもよい。また、画像データの色情報、明度、彩度に関する情報など、画像毎に異なる情報を画像識別情報IDとしてもよい。

【0054】画像情報通知部26は、暗号作成部22が作成したデジタル署名の復号化方法、電子透かし合成部24が合成した電子透かしの抽出方法、及び暗号作成部22がデジタル署名を作成するときに用いた画像識別情報IDを、工事の発注者又は画像改ざん判定装置90に通知する。通知手段として電子メールや郵便等を用いることができる。

【0055】図4は、電子透かし合成方法のフローチャートである。本図を参照しながら、電子透かし合成装置80が行う電子透かし合成方法を説明する。

【0056】画像入力部10は画像を入力する(S200)。暗号作成部22は、画像識別情報IDに対して、秘密鍵sk及び復号化関数Dを用いてデジタル署名D(ID, sk)を作成する(S202)。

【0057】電子透かし合成部24は、暗号作成部22が作成したデジタル署名を電子透かしとして画像入力部10が入力した画像に合成する(S204)。電子透かしの画像に合成する方法及び合成された電子透かしを画像から抽出する方法は、「電子透かしの基礎〜マルチメディアのニュープロテクト技術〜」(松井甲子雄著、森北出版)に記載された方法を用いることができる。

【0058】記録部40は、電子透かし合成部24が合成した画像をCD-ROMなどの記録媒体に記録する(S206)。

【0059】電子透かし合成装置80を用いて合成された画像は、記録部40によってCD-ROMなどに格納されて受注者に渡される。

【0060】受注者はCD-ROMに格納された画像を選択して、工事を説明する写真データとして発注者に提出する。発注者は、受注者が提出した画像から電子透かしを抽出し、抽出された電子透かしをデジタル署名の復

号化方法にしたがって、復号化する。電子透かしがデジタル署名D(ID, sk)であるとき、復号されたデータは、E(D(ID, sk), pk)である。E(D(ID, sk), pk)が、先にラボシステムから通知された画像識別情報IDに等しいかどうかを調べ、改ざんの有無を検出する。

【0061】受注者は画像に埋め込まれた電子透かしを見破ることは困難である。仮に受注者が画像データを改ざんした場合、画像に埋め込まれた電子透かしの情報が壊れる。そのため、発注者が改ざんされた画像データから電子透かし情報を抽出し、デジタル署名を取り出し、デジタル署名を復号化しても画像識別情報IDが正しく復元されない。したがって発注者は、ラボシステムの管理者から通知された画像識別情報と比較して、画像データが改ざんされたことを知ることができる。

【0062】仮に受注者がデジタル署名の作成に使用した画像識別情報IDを知っても、公開鍵暗号系を用いたデジタル署名の場合、秘密鍵を知らない限りはデジタル署名を作成することができない。したがって、受注者が自ら画像識別情報IDからデジタル署名を作成して、画像に電子透かしとして埋め込むことはできない。

【0063】画像識別情報IDとして、受注者識別情報を使用した場合、受注者毎にデジタル署名が同じになる。画像識別情報IDとして、注文識別情報を使用した場合、同一の受注者であっても、注文単位毎にデジタル署名が変わる。そのため、受注者が電子透かしとして埋め込まれたデジタル署名を見破ることは困難になる。

【0064】画像識別情報IDとして、画像データ毎に異なる識別情報を用いた場合、デジタル署名は画像毎に一つ一つ異なるため、受注者が電子透かしとして画像に埋め込まれたデジタル署名を見破ることは一層困難になり、改ざんを防止する効果を高めることができる。

【0065】図5は、本発明の第2の実施形態に係る画像改ざん判定装置90の構成図である。画像改ざん判定装置90は、画像入力部11と、画像情報入力部12と、処理部60と、出力部50とを有する。

【0066】画像入力部11は、記録媒体に格納された画像を入力する。フロッピーディスク、MO、CD-ROM等から画像データを読み取る場合は、画像入力部10としてそれぞれフロッピードライブ、MOドライブ、CDドライブ等が用いられる。

【0067】画像情報入力部12は、画像入力部11が入力する画像に関して、電子透かしを抽出する方法、暗号情報復号方法の一例として、デジタル署名の暗号を復号する方法、及び画像識別情報IDを入力する。

【0068】処理部60は、画像入力部10が入力する画像の電子透かしを抽出し、抽出した電子透かしをデジタル署名として、デジタル署名を復号化し、画像識別情報を抽出し、改ざんの有無を判定する。

【0069】出力部50は、処理部20から受け取った



画像を出力する。例えば画像を画面表示する場合、出力部50には画像を表示するモニタが用いられる。

【0070】図6は、処理部60の機能ブロック図である。処理部60は、電子透かし抽出部62と、暗号復号部64と、改ざん判定部66とを有する。

【0071】電子透かし抽出部62は、画像情報入力部12が入力した電子透かし抽出方法を用いて、画像入力部10が入力した画像から電子透かしを抽出する。暗号復号部64は、抽出された電子透かしをデジタル署名とみなし、画像情報入力部12が入力したデジタル署名の復号方法を用いて、デジタル署名を復号化する。改ざん判定部66は、暗号復号部64が復号化して得られたデータと、画像情報入力部12が入力する画像識別情報IDとが一致するかどうかを検出することにより、改ざんの有無を判定する。

【0072】図7は、画像改ざん判定方法のフローチャートである。本図を参照しながら、画像改ざん判定装置90が行う画像改ざん判定方法を説明する。

【0073】画像入力部11は画像を入力する(S220)。画像情報入力部12が、画像入力部10が入力した画像に関する、電子透かし抽出方法、デジタル署名復号方法及び画像識別情報IDを入力する(S222)。

【0074】電子透かし抽出部62は、画像情報入力部12が入力した電子透かし抽出方法に基づいて画像から電子透かしを抽出する(S224)。暗号復号部64は、電子透かし抽出部62が抽出した電子透かしをデジタル署名 $D(ID, sk)$ の値であるとみなし、公開鍵 $pk$ を用いて復号化する。暗号復号部64は、画像情報入力部12が入力する復号方法から暗号化関数 $E$ を知り、公開鍵 $pk$ を用いて暗号化関数 $E$ により、デジタル署名 $D(ID, sk)$ を復号化し、復号化データとして $E(D(ID, sk), pk)$ を得る(S226)。

【0075】改ざん判定部66は、暗号復号部64が復号化したデータ $E(D(ID, sk), pk)$ が、画像情報入力部12が入力する画像識別情報IDに等しいかどうかを調べる(S228)。もし等しいなら、画像は改ざんされていないと判定し(S230)、もし等しくないなら、画像は改ざんされていると判定する(S232)。

【0076】本実施形態の画像改ざん検出装置によれば、受注者が発注者に提出する画像から電子透かしを抽出し、電子透かしをデジタル署名とみなし、復号化することによって画像識別情報を取り出すことができる。得られた画像識別情報を、先にラボシステムの管理者から通知された画像識別情報と照合することにより、画像の改ざんの有無を検出することができる。

【0077】図8は、本発明の第3の実施形態に係る画像改ざん判定装置の構成図である。本実施形態の画像改ざん判定装置の基本的な構成及び動作は、図5で示した第2の実施形態の画像改ざん判定装置と同様である。本

実施形態では、画像改ざん判定装置の処理部60として、パーソナルコンピュータやワークステーション等の電子計算機を用いる点が、第2の実施形態と異なる。

【0078】図8を参照しながら、処理部60のハードウェア構成を説明する。CPU30はROM32及びRAM34に格納されたプログラムに基づいて動作する。キーボード、マウス等の入力装置31を介して利用者によりデータが入力される。ハードディスク33は、画像等のデータ、及びCPU30を動作させるプログラムを格納する。CD-ROMドライブ35はCD-ROM100からデータ又はプログラムを読み取り、RAM34、ハードディスク33及びCPU30の少なくともいずれかに提供する。

【0079】処理部60のCPU30が実行するソフトウェアの機能構成は、図6と同じであり、電子透かし検出モジュール162と、暗号復号モジュール164と、改ざん判定モジュール166とを有する。

【0080】電子透かし検出モジュール162、暗号復号モジュール164、及び改ざん判定モジュール166がコンピュータに働きかけて、CPU30に行わせる処理は、それぞれ図6に示した、第2の実施形態の画像改ざん判定装置90における、電子透かし抽出部62、暗号復号部64、及び改ざん判定部66の機能及び動作と同一であるから、説明を省略する。これらのソフトウェアは、CD-ROM100等の記録媒体に格納されて利用者に提供される。ソフトウェアは記録媒体からハードディスク33にインストールされ、RAM34に読み出されてCPU30により実行される。

【0081】記録媒体の一例としてのCD-ROM100には、本出願で説明した処理部20又は処理部60の動作の一部又は全ての機能を格納することができる。またCD-ROM100には他の装置の動作の一部又は全ての機能を格納することができる。これらのプログラムは記録媒体から直接RAM34に読み出されて実行されてもよい。

【0082】記録媒体としては、CD-ROM100の他にも、DVDやPD等の光学記録媒体、フロッピーディスクやミニディスク(MD)等の磁気記録媒体、MO等の光磁気記録媒体、テープ状記録媒体、不揮発性の半導体メモリカード等を用いることができる。上記のプログラムを格納した記録媒体は、電子透かし合成装置及び画像改ざん判定装置を製造するためにのみ使用されるものであり、そのような記録媒体の業としての製造および販売等が本出願に基づく特許権の侵害を構成することは明らかである。

【0083】以上述べたように、第1の実施形態の電子透かし合成装置によれば、受注者の写真の画像データに対して、画像識別情報に対するデジタル署名を作成し、電子透かしとして画像に合成することができる。

【0084】受注者が画像の改ざんを行うと、電子透か



しの情報が壊れるため、改ざんの形跡を画像に残すことができる。合成された電子透かしは受注者が容易に取り出すことができない。仮に電子透かしが抽出されたとしても、抽出された電子透かしは画像識別情報のデジタル署名であり、容易に復号化することができない。

【0085】画像識別情報として、受注者毎に異なる情報、注文毎に異なる情報、及び画像毎に異なる情報を使い分けることにより、電子透かしとして埋め込まれたデジタル署名のセキュリティの強さを変えて、改ざんの防止の効果を向上させることができる。

【0086】第2の実施形態の画像改ざん検出装置によれば、受注者が発注者に提出する画像から電子透かしを抽出し、電子透かしをデジタル署名とみなし、復号化することによって画像識別情報を取り出すことができる。得られた画像識別情報は、先にラボシステムの管理者から通知された画像識別情報と照合され、画像の改ざんの有無を検出することができる。

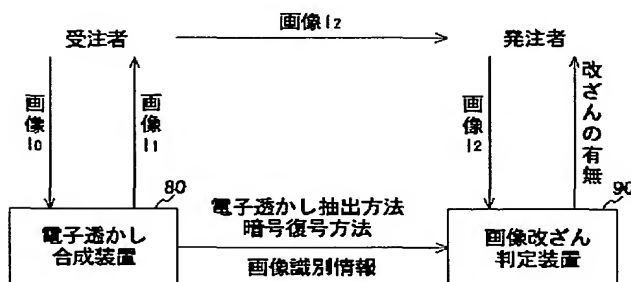
【0087】以上、本発明を実施の形態を用いて説明したが、本発明の技術的範囲は上記実施の形態に記載の範囲には限定されない。上記実施の形態に、多様な変更又は改良を加えることができることが当業者に明らかである。その様な変更又は改良を加えた形態も本発明の技術的範囲に含まれ得ることが、特許請求の範囲の記載から明らかである。

【0088】

【発明の効果】上記説明から明らかなように、本発明によれば、発注者の依頼に基づいて受注者が撮影した画像に電子透かしを合成し、受注者が発注者に提出する画像の改ざんの有無を判定することができる。

【図面の簡単な説明】

【図1】



【図1】 本発明の電子透かし合成装置80と画像改ざん判定装置90を用いて、画像の改ざんの有無を判定するシステムの構成図である。

【図2】 本発明の第1の実施形態に係る電子透かし合成装置80の構成図である。

【図3】 処理部20の機能ブロック図である。

【図4】 電子透かし合成方法のフローチャートである。

【図5】 本発明の第2の実施形態に係る画像改ざん判定装置90の構成図である。

【図6】 処理部60の機能ブロック図である。

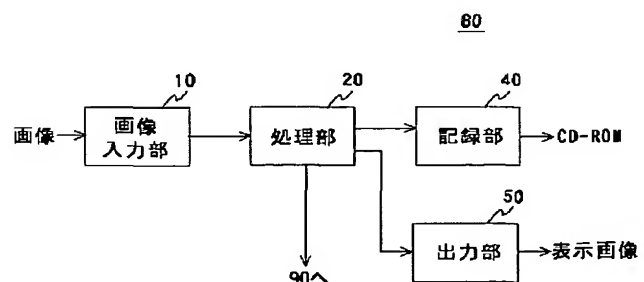
【図7】 画像改ざん判定方法のフローチャートである。

【図8】 本発明の第3の実施形態に係る画像改ざん判定装置の構成図である。

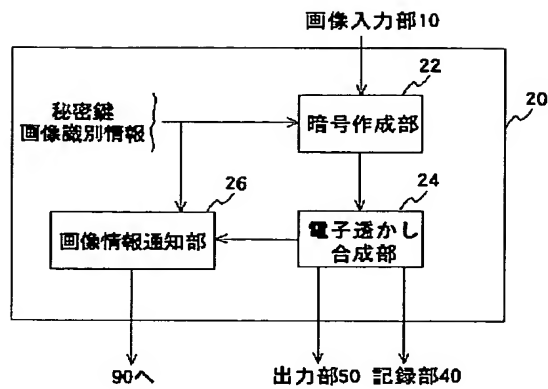
【符号の説明】

10	画像入力部	12	画像情報入力部
20	処理部	22	暗号作成部
24	電子透かし合成部	26	画像情報通知部
40	記録部	50	出力部
60	処理部	62	電子透かし抽出部
64	暗号復号部	66	改ざん判定部
80	電子透かし合成装置	90	画像改ざん判定装置

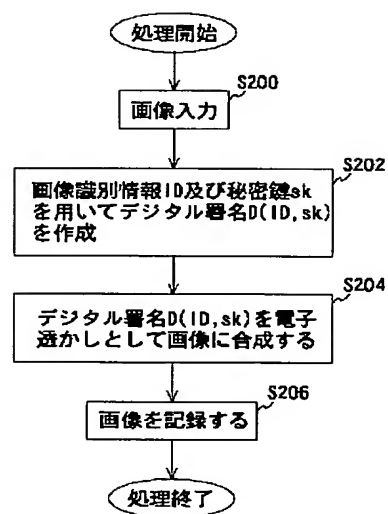
【図2】



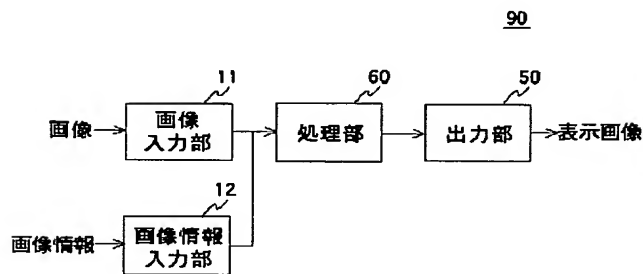
【図3】



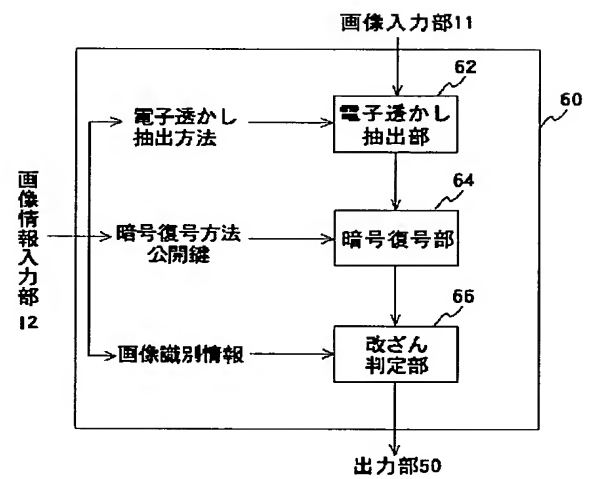
【図4】



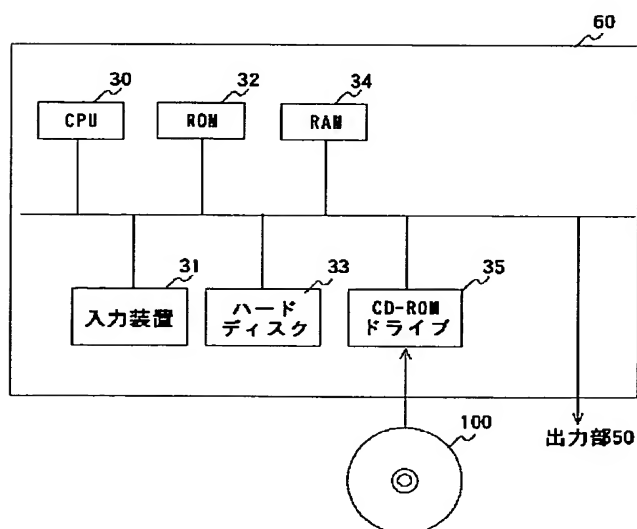
【図5】



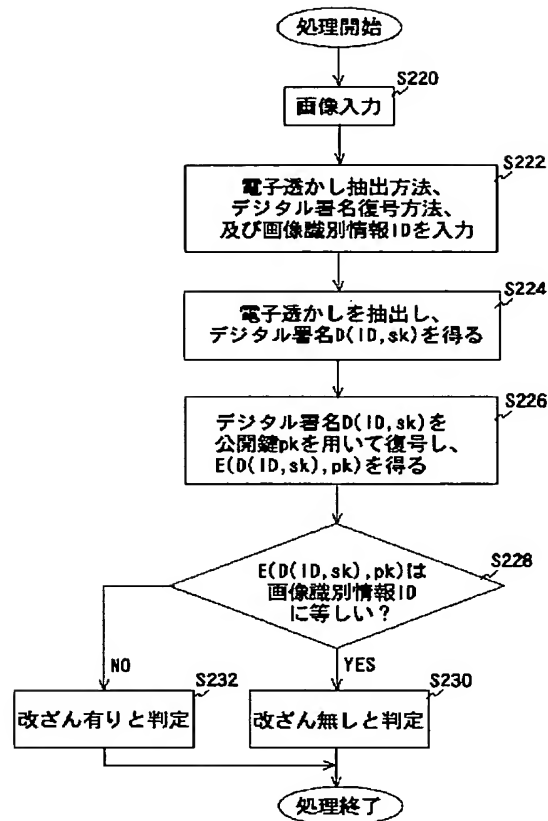
【図6】



【図8】



【図7】



フロントページの続き

(51)Int.Cl.<sup>7</sup>  
H 0 4 L 9/32

識別記号

F I  
H 0 4 L 9/00

テーマコード(参考)

6 7 3 E

Fターム(参考) 5B057 AA20 CE08  
5C076 AA14 BA06  
5J104 AA07 AA09 AA14 KA01 KA05  
LA03 LA06 NA02 NA05 NA29  
NA32 PA14